Adversary Threat Tactics are Changing

<u>Early 2010s</u>

Zero-day Vulnerabilities

(Nation State, Industrial Espionage, Black Market)

<u>Today</u>

Rapidly weaponizing newly-disclosed vulnerabilities
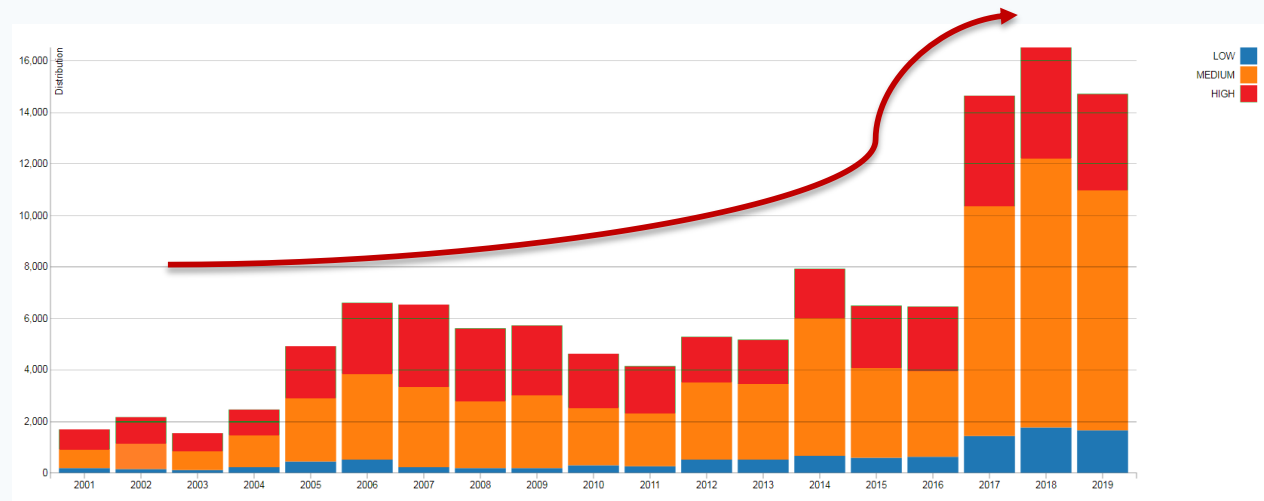*(Good, Fast, Cheap – Pick 3)*

Qualys.

Known Critical Vulnerabilities are Increasing

14-16K vulnerabilities are disclosed 2017-2019

30-40% are ranked as "High" or "Critical" severity

Worm-able Vulnerabilities are increasing (WannaCry, BlueKeep)

"Mean Time to Weaponize" is rapidly decreasing year/year

Qualys.

Let's Talk About BlueKeep
(RDP Vulnerability)

U.S. Govt Achieves BlueKeep Remote Code Execution, Issues Alert

By **Sergiu Gatlan**

📅 June 17, 2019   ⏰ 11:13 AM   💬 1

US company selling weaponized BlueKeep exploit

An exploit for a vulnerability that Microsoft feared it may trigger the next WannaCry is now being sold commercially.

By Catalin Cimpanu for Zero Day | July 25, 2019 -- 09:06 GMT (02:06 PDT) | Topic: Security

7/30/2019
12:00 PM

BlueKeep Exploits Appear as Security Firms Continue to Worry About Cyberattack

The lack of an attack has puzzled some security experts, but the general advice remains that companies should patch their vulnerable systems more quickly.

Robert Lemos

Just Two Weeks Ago

Windows 'BlueKeep' Attack That U.S. Government Warned About Is Happening Right Now

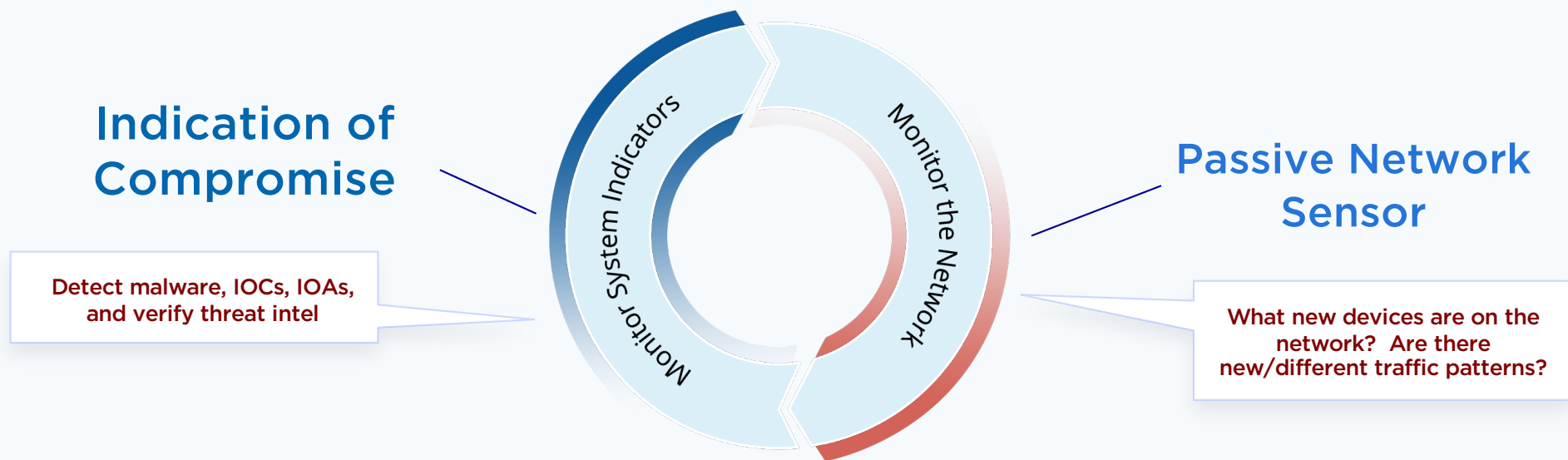**Davey Winder** Senior Contributor ⓘ

Cybersecurity

I report and analyse breaking cybersecurity and privacy stories

Get Proactive – Reduce the Attack Surface

AI **VM** Immediately discover assets and vulnerabilities

PM Notify IT asset owner to patch / stop the instance

PC **SCA** Change configuration to limit unauthorized access

CSA Control network access / cloud security groups

IOC Add endpoint detection and response

Qualys.

Proactively Hunt, Detect, and Respond

Indication of Compromise

Detect malware, IOCs, IOAs, and verify threat intel

Monitor System Indicators

Monitor the Network

Passive Network Sensor

What new devices are on the network? Are there new/different traffic patterns?

Qualys.

Qualys IOC – Hunt Using Threat Intel

1 Threat intelligence lists attack information …

2 Search for the file hash here…

3 Find the object there.

Detect Malware Missed by Anti-Virus

UK Government Contractor

- "Big 4" anti-virus installed
- Qualys Agent for Vulnerability Mgmt
- Added Qualys IOC on existing agents
- 256 hosts

Qualys IOC discovered...

- Dridex Banking Trojan (51)
- 4 domain controllers infected
- Backdoors (7) installed due to phishing campaigns
- Netcat (8) root kits installed
- 46 PUAs installed
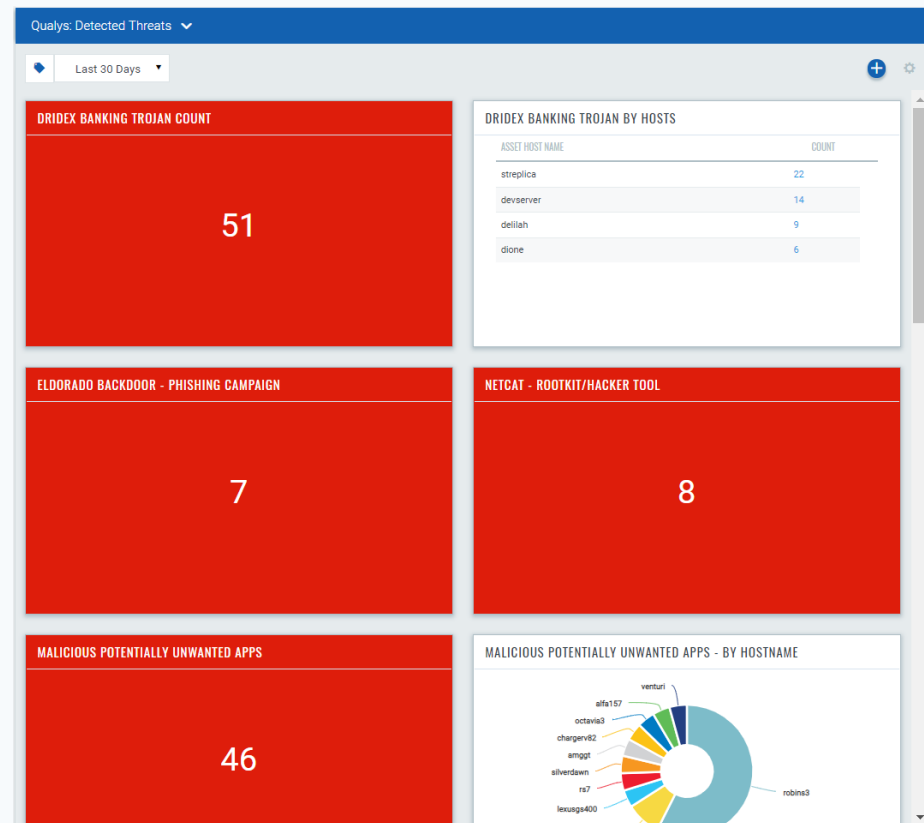
Demo

9aa730979342f8d719e730f1a2081d8e9852da646ce2fbd9ce5e5301de25a5c5

Beyond Endpoint Detection and Response: How can I better protect my crown jewels?

Threat Hunting Assumptions:

- Every user machine can be compromised – it only takes one

- Every Remote Code Execution (RCE) vulnerability can be exploited

- Local Privilege Escalation and Credential Harvesting to move laterally

- System misconfigurations are often overlooked and easy to exploit

- Network segmentation is rarely used internally due to management

- All attacks are not equal: can Adversaries reach my Critical Servers?

Qualys.

Adversary Lateral Movements (Attack Paths)

Security Tiers

lower ← → *higher*

User Segments

Business Apps / IT Systems

**Tier 0 Systems
"Crown Jewels"**

2 Find systems in higher security tiers by looking for existing connections or network reconnaissance.

1 Bad actor compromises a user machine (email, phishing, watering hole, etc.).
Takes remote control of the machine.

3 Laterally move to new system by:
- Exploiting open vulnerabilities
- Take advantage of misconfigurations
- Use compromised credentials

4 Laterally move to new system by:
- Exploiting open vulnerabilities
- Take advantage of misconfigurations
- Use compromised credentials

Qualys.

Finding Attack Paths

Network Reachability

Determine connections between hosts using Cloud Agent **CA**

Passive + Active network collection

Store these connections in a Graph Database for fast query

\+

Asset Security Posture

Remote Code Execution Vulnerabilities **VM** **TP**

System Misconfigurations **PC** **SCA**

Malware and Indicators of Activity **IOC**

Qualys.

Attack Path Discovery
to
Prioritize Patching and
Improve Security Defenses

Hunting

5	✕ 5ceec909f3dfc890fdd1e76d6f3cc093465c9d980d68b9987fc3f5eb289b6bd2
Total Events	Active View ▾ ☰

1 - 5 of 5   ◁▷ ⬇ ↻ ⚙

TIME ▾		OBJECT		ASSET	SCORE	DETAILS
21 hours ago 12:58:21 AM	⇄	**66.85.173.57 (tar.theoutlan.com) : 443** TCP CONNECTION - ESTABLISHED by temp0291.exe	⊞	**SHAREPT003** 172.31.0.111	**10**	**Trickbot** Trojan
a day ago 8:19:31 PM	📄	**temp0291.exe** c:\Users\qualys\AppData\Roaming	⊞	**SHAREPT003** 172.31.0.111	**8**	**Trickbot** Trojan
a day ago 3:12:28 PM	⚙	**temp0291.exe** C:\Users\qualys\AppData\Roaming\temp0291.exe	⊞	**SHAREPT003** 172.31.0.111	**9**	**Trickbot** Trojan
a day ago 3:02:08 PM	🔒	**\BaseNamedObjects\4C3D653494D1128** temp0291.exe	⊞	**SHAREPT003** 172.31.0.111	**9**	**Trickbot** Trojan
2 days ago 11:18:23 AM	📄	**temp0291.exe** c:\Users\qualys\AppData\Roaming	⊞	**SHAREPT003** 172.31.0.111	**8**	**Trickbot** Trojan

TYPE

file	2
mutex	1
network	1
process	1

EVENT ACTION

created	2
established	1
running	2

SCORE

10	1
9	2
8	2

Network

Topology · List View

Search · Last 7 days ▾

Group Assets by... ▾

172.16.201.44

Attack path leads to this critical server

172.16.201.93
172.16.201.113
172.16.201.23
172.16.201.56
172.16.201.68
172.16.201.22
172.16.201.70
172.16.201.88
172.16.201.11

shippinglabelApp
HMI:MM5

HMI:GE
HR SharePoint
172.16.201.13
172.16.201.99

Flex IO
HP LaserJet 400 MFP M425 Postscript

172.16.201.93
Site 1

Qualys.
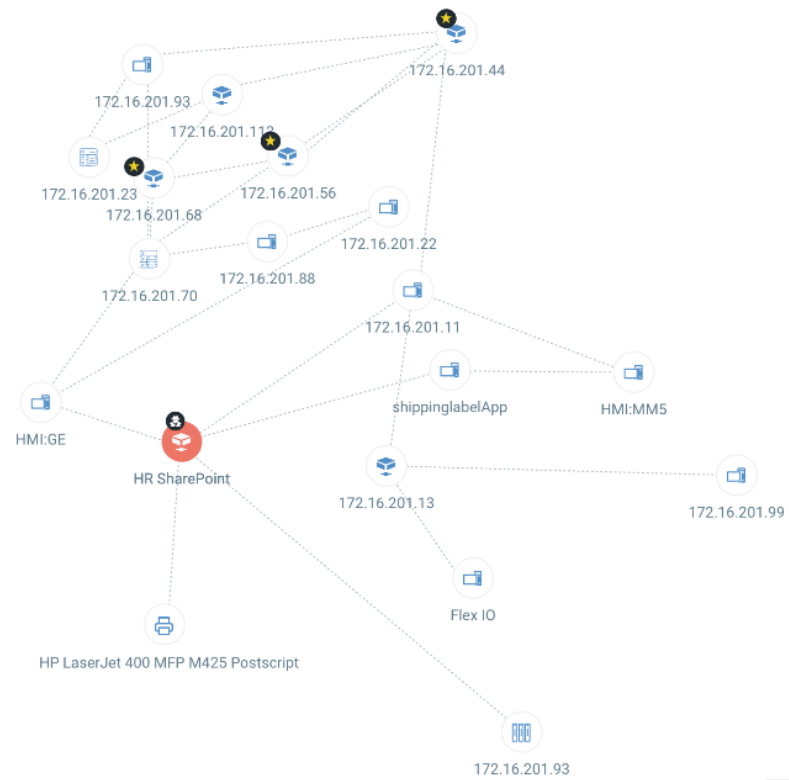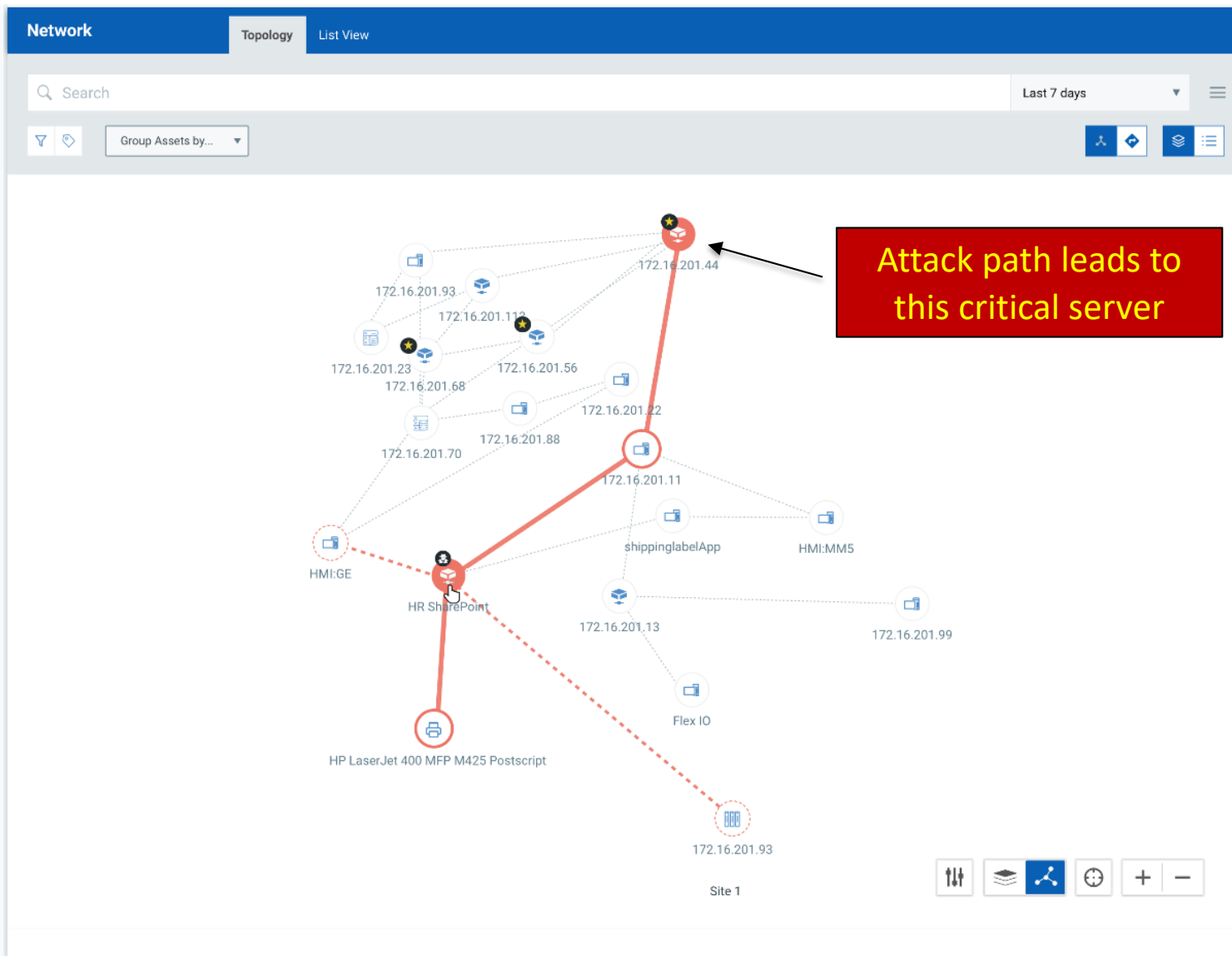
Network   Topology   List View

Search

Group Assets by... ▼

172.16.201.44

172.16.201.93
172.16.201.112
172.16.201.23
172.16.201.68   172.16.201.56
172.16.201.70   172.16.201.88
172.16.201.22
172.16.201.11

HMI:GE
shippinglabelApp   HMI:MM

HR SharePoint
172.16.201.13

HP LaserJet 400 MFP M425 Postscript

Flex IO

172.16.201.93

Site 1

Actions ▼

HR SHAREPOINT
172.31.0.111
New York, NY

Tags
New York Corporate Apps HR Apps
Share Point 60_day_lastscan

⌃ **INFECTIONS** (4 Events)

Process: temp0294.exe   Quick Menu ▼
Malware: Trickbot | Risk Scor
                                        View Asset Details
File: WormDll64   Execute a Response
Malware: Trickbot | Risk Sco   Quarantine Host

File: NetworkDll64   ⋮
Malware: Trickbot | Risk Score: 8

File: ShareDll64   ⋮
Malware: Trickbot | Risk Score: 8

Take action on this
host to stop the
attacker in their tracks

Qualys.

Breach Attack & Simulation ▾

DASHBOARD   ASSETS   NETWORK   SCANS   CONFIGURATION

Network

Q Search

▽ ◌   Group As

Execute a Response

The following response will be executed for the selected processes and files on the defined hosts.

Process (1)

RISK SCORE	PROCESS NAME	MALWARE	PID	HOST
9	temp0291.exe	TrickBot	4417	SHAREPT003

☑ Kill Process   ☑ Quarantine File

File Type (3)

RISK SCORE	FILE NAME	MALWARE	HOST
8	WormDll64 (C:\Users\support\AppData\Roaming)	TrickBot	SHAREPT003
8	NetworkDll64 (C:\Users\support\AppData\Roaming)	TrickBot	SHAREPT003
8	ShareDll64 (C:\Users\support\AppData\Roaming)	TrickBot	SHAREPT003

☑ Quarantine File

Cancel   Confirm

172.16.201.93

Site 1

Qualys.

Scale Human Response with Automation

Find active attacks on endpoint using Indication of Compromise

Go beyond endpoint detection with Security Analytics – correlate user, network, application, cloud, container

Use attack path discovery as metadata to detect active attacks reaching critical assets

Automate response to protect critical assets using response playbooks
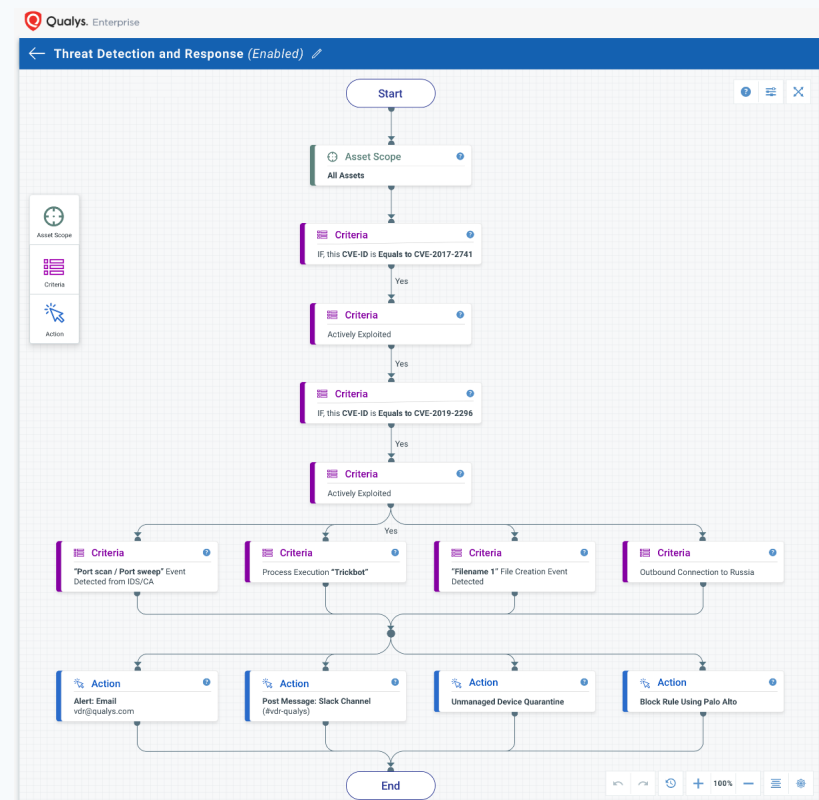
Thank You

Chris Carlson
ccarlson@qualys.com